NP - 4
NC - 28
PN - EP-991242 A2 20000405 DW2000-22 H04L-029/06 Eng 13p *
AP: 1999EP-0307615 19990928
DSR: AL AT BE CH CY DE DK ES FI FR GB GR IE IT LI LT LU LV MC MK NL PT RO SE SI
- JP2000148685 A 20000530 DW2000-33 G06F-015/00 13p
AP: 1999JP-0274268 19990928
- CN1249590 A 20000405 DW2000-34 H04L-009/32
AP: 1999CN-0120534 19990929
- KR2000028722 A 20000525 DW2001-10 H04L-009/32
AP: 1999KR-0041523 19990928
PR - 1998US-0163050 19980929
IC - G06F-015/00 H04L-009/32 H04L-029/06 G06F-012/00 G06F-017/60 H04L-012/22 H04L-012/28 H04L-012/54 H04L-012/58
AB - EP-991242 A
NOVELTY - The method involves a set of client devices communicating using a wireless network to access web servers (205-207), available on the Internet, within a protected realm which requires credentials. A credential caching proxy server intercepts and caches a client's credentials when a credential is sent from the wireless user agent to a protected server. The cached credential is used for all subsequent requests to web servers within the same protected realm.
- DETAILED DESCRIPTION - An INDEPENDENT CLAIM is included for
- (1) an apparatus for caching credential information within a communication system
- USE - For caching credentials in proxy servers used by wireless client devices when accessing protected resources. For mobile telephone accessing information on the Internet.
- ADVANTAGE - Reduces number of bits and bytes that must be transmitted over the low bandwidth and expensive wireless communication infrastructure since a credential does not need to be sent for every request into a protected realm.
- DESCRIPTION OF DRAWING(S) - The figure shows a functional diagram of an Internet proxy system for wireless client device where a credential cache is provided.
- Web servers 205-207(Dwg.2/3)
MC - EPI: W01-A03B W01-A05A W01-A06B7 W01-A06E1 W01-A06E2A W01-A06F W01-A06G2 W01-B05A1A W01-C02B6A W02-C03C1A
UP - 2000-22
UE - 2000-33; 2000-34; 2001-10

3/4 DWPI - (C) Derwent- image
AN - 2000-180614 [16]
XP - N2000-133246
TI - Servlet/Applet/HTML authentication process with single sign-on employs authentication data encrypted single sign-on cookie to provide secure Servlets
DC - T01
PA - (IBMC ) INT BUSINESS MACHINES CORP
NP - 1
NC - 1
PN - RD-429128 A 20000110 DW2000-16 G06F-000/00 3p *
AP: 1999RD-0429128 19991220
PR - 1999RD-0429128 19991220
IC - G06F-000/00

AB - RD-429128 A
NOVELTY - The process begins when a user uses their web browser to request content (such as a user's personal home page) from a content Servlet. The content Servlet will attempt to retrieve an SSO cookie from the web browser. If the cookie is not found, or its timestamp indicates that it has expired, the Servlet begins the login process.
- DETAILED DESCRIPTION - Otherwise, the Servlet will use the authentication data encrypted in the cookie to authenticate the user in the Servlet's JVM. If this authentication fails, the Servlet will begin the login process. If it succeeds, it will send the content the user requested (the home page).
- USE - For authentication of Servlet/Applet/HTML.
- ADVANTAGE - (a) The user will not have to log in twice if the Java login Applet is used. The login Applet logs the user in to the Applet JVM, so all Applets later launched in that JVM will recognize the user as being logged in. Then the Applet sends a request to the login Servlet to continue the process; (b) Java and JavaScript are not required. If the user (or system administrator) does not expect to use authenticated Java Applets, the HTML login form can be used. This will log the user in with a Servlet and set the Single Sign-On cookie. This login process only requires a web browser that supports cookies and secure connections via HTTPS; (c) Using a minimum of Java makes web-based applications more flexible and more likely to run in a wide variety of web browsers on a variety of platforms. Web browsers often implement Java differently, which sometimes necessitates browser-specific code. This code makes web applications more fragile and buggy, and it prevents them from being used with browsers or platforms that were not tested with them while they were being developed; (d) Less memory is used on the client in most cases. If the HTML login Is used, no Java classes are loaded on the client. The login Applet loads only a minimal set of Java class archives (significantly less than the ODS Applet Launcher). Any other Applets load additional class archives only as they are needed; (e) Configurable security. The user name and password are always sent over secure connections. The SSO cookie in the web browser is encrypted so it cannot be read easily. The domains which can retrieve the SSO cookie are administrator-controlled, so it can only be retrieved by trusted servers. In case the cookie is stolen from the network, it expires after an amount of time chosen by the ODS administrator. Other Servlets will respond via either HTTP or HTTPS, depending on the system administrator's preference. Applets are loaded via HTTP for technical reasons, but they always communicate back to the server via HTTPS or secure RMI; (f) Single Sign-On can also authenticate the user to use other web applications that support SSO.
- DESCRIPTION OF DRAWING(S) - The diagram shows an overview of the authentication process. (Dwg.1/1)
MC - EPI: T01-D01 T01-H07C5A T01-J11C1
UP - 2000-16

4/4 DWPI - (C) Derwent- image
AN - 1999-171619 [15]
XP - N1999-125642
TI - Security management method of client server networks - involves using certificates and unique IDs issued by authentication server to ensure secured communication
DC - T01 W01